基于 Curvelet-DSVD 和视觉密码的强鲁棒零水印算法 *

曲长波，吴德阳

(辽宁工程技术大学 软件学院，辽宁 葫芦岛 125105)

摘 要：为了更好的表现自然图像的曲线特性，进一步提高数字水印算法的鲁棒性，提出一种基于 Curvelet-DSVD 和视觉密码相结合的强鲁棒零水印算法。首先对原始图像进行 Arnold 置乱；其次进行 Curvelet 变换得到低频域信息，对低频域信息进行分块并对各个块进行双奇异值分解(DSVD)，利用块最大奇异值与整体奇异值均值之间的关系构造特征矩阵，同时利用视觉密码将水印信息生成两个共享份；最后将其中一个共享份进行 Arnold 置乱后与特征矩阵进行异或运算生成零水印。实验结果表明，该算法能够有效地抵抗常规攻击，与现有的零水印算法相比，鲁棒性更强，安全性更高。

关键词：Curvelet 变换；双奇异值分解；视觉密码；鲁棒性

中图分类号：TP309.2　　doi: 10.3969/j.issn.1001-3695.2017.10.0936

Strong robust zero watermarking algorithm based on Curvelet - DSVD and visual cryptography

Qu Changbo, Wu Deyang

(*College of Software Liaoning Technical University*, *HuLudao Liaoning* 125105, *China*)

Abstract: In order to better perform the characteristics of natural image curves and further improve the robustness of digital watermarking algorithms, this paper proposed a robust zero-watermarking algorithm based on Curvelet-DSVD and visual cryptography. Firstly, performing Arnold scrambling on the original image, then obtaining the low frequency domain information by Curvelet transform, segmenting the low frequency domain information, and each block was double singular value decomposition(DSVD) , by using the relationship between the maximum singular value of the block and the mean value of the global singular value structuring characteristic matrix. At the same time, this paper used the visual cryptography to generate two shared copies of the watermark information. Finally, one of the shares was execute to Arnold scramble and then xor operation with the feature matrix to generate a zero-watermark. Experimental results show that the proposed algorithm can effectively resist the conventional attacks and is more robust and more secure than the existing zero-watermarking algorithms.

Key Words: curvelet transform; double singular value decomposition (DSVD); visual cryptography; robustness

0 引言

为了解决传统变换域水印算法的透明性与鲁棒性之间的矛盾，温泉等人[1]提出零水印的概念，由于零水印算法不需要将版权信息嵌入到载体图像中，对载体图像的内容完整性起到很好的保护作用，所以近年来零水印在版权保护领域得到广泛的应用[2,3]。

传统的零水印算法大都利用小波变换和奇异值分解构造载体图像的特征信息，然后与水印信息结合生成零水印[4~6]。文献[4]利用离散小波和奇异值分解构造零水印，对于小范围的噪声攻击、滤波攻击和压缩攻击具有较好的稳定性，但对于较大强度的攻击鲁棒性较差。文献[5]提出一种基于不变质心的鲁棒零水印算法，选择不变质心作为稳定的几何参考点，能够有效的抵抗几何攻击的影响，但滤波攻击和噪声攻击对构造的特征矩阵产生一定影响。文献[6]提出一种基于 DWT-SVD 的图像双零水印算法，利用 haar 小波对载体图像进行两次变换，选择载体图像的低频域 LL2 来构造零水印。随着对水印算法的不断研究，近年来出现许多较为新颖的水印算法[7~9]，文献[7]选取图像感兴趣的区域构造特征矩阵，再将特征矩阵与水印图像进行异或运算生成零水印。算法对于常规攻击具有一定的鲁棒性，但当感兴趣域受到攻击时，水印信息影响较大，具有一定的局限性。文献[8]利用余弦离散小波变换（DCT）具有能量集中优势来构造零水印，但利用图像块均值构造特征矩阵稳定性较差。为提高图像特征的稳定性，曾文权等人[9]利用整数小波变换和混沌加密原理提出一种基于整数小波变换的鲁棒零水印算法。实验结果表明算法对于非几何攻击具有较强的鲁棒性，但由于算法

基金项目：国家自然科学基金资助项目（61404069）

作者简介：曲长波（1963-），男，高级工程师，硕导，主要研究方向为图像处理、信息隐藏、网络安全（fx_qcb@126.com）；吴德阳（1992-），男，硕士研究生，主要研究方向为图像处理、数字水印、信息安全.

未考虑几何攻击对图像的影响，所以在受到剪切攻击和旋转攻击时，提取的水印相似度较低。为了克服几何攻击对载体图像的影响，曲长波等人[10]利用小波变换结合视觉密码提出一种基于视觉密码和边缘检测的零水算法。算法对于小范围的噪声攻击具有较好的鲁棒性，但对于几何攻击表现鲁棒性较差。肖振久等人[11]提出了一种基于增强奇异值分解和细胞神经网络的零水印算法，算法通过均匀化奇异值并结合神经网络算法解决了对角线失真问题，但神经网络的引入，增加了算法的时间复杂度。以上算法虽然使用小波变换能够很好地将图像分为高频域和低频域，但是自然图像中包含有大量的纹理特征，曲线奇异性表现比较突出,小波变换对于点奇异特性表现较好，而对于图像曲线奇异特性表现较差，所以在受到攻击时提取的水印信息往往影响比较大。

针对上述问题，本文提出一种基于 Curvelet-DSVD 和视觉密码的强鲁棒零水印算法。首先对载体图像进行 Arnold 置乱；其次对置乱后的载体图像进行 Curvelet 变换提取出图像曲线特征信息，并对得到的曲线信息的进行分块和 DSVD；然后利用块最大奇异值与块整体最大奇异值的均值之间的关系构造特征矩阵，同时对水印图像进行视觉密码加密操作，产生两个秘密图份，将其中一个秘密图份进行 Arnold 置乱，将特征矩阵与置乱后的秘密图份进行异或操作生成零水印；最后将生成的零水印与另一秘密图份保存至版权保护中心。

1 基础理论

1.1 Curvelet 变换理论

Curvelet 变换是一种多分辨、带通、具有方向性的函数分析方法，是通过一种特殊的滤波过程和多尺度 Ridgelet 变换来实现的，对于图像曲线边缘的描述，其逼近性能具有近乎最优的非线性逼近误差衰减阶，对曲线特征信息具有很好的表示性能[12]。以笛卡尔坐标系下的 $f[t_1,t_2](0\le t_1,t_2<n)$ 作为输入，Curvelet 变换的离散形式为

$$c^D(j,l,k):=\sum_{0\le t_1,t_2<n} f[t_1,t_2]\overline{\phi^D_{j,l,k}[t_1,t_2]} \tag{1}$$

其中：$j\in 0,1,2,3\cdots n$ 为尺度参数；$l\in 0,1,2,3\cdots n$ 为方向参数；$k=(k_1,k_2)\in Z^2$ 是一个旋转参数。Canddes 和 Donoho 提出了一种基于 USFFT(unequally spacefast Fourier trans form)的快速离散 Curvelet 变换实现方法[12]，步骤如下：

a) 对于给定一个笛卡尔坐标下的二维函数进行 2DFFT 变换，得到二维频域信息。

$$\hat{f}[n_1,n_2],-n_1/2,n_2/2 \tag{2}$$

b) 对得到的二维频域信息进行重采样，得到相应的采样值。

$$\hat{f}[n_1,n_2-n_1\tan\theta_l],(n_1,n_2)\in P_j \tag{3}$$

c) 将内插后的 $\hat{f}$ 与 $\hat{U}$ 函数相乘得到 $\hat{f}[n_1,n_2]$

$$\hat{f}[n_1,n_2]=\hat{f}[n_1,n_2-n_1\tan\theta_l]\tilde{U}_j[n_1,n_2] \tag{4}$$

对 $\tilde{f}_{j,l}$ 进行 IFFT 逆变换得到离散 Curvelet 变换的系数集合 $c^D(j,l,k)$。

图 1 是 Curvelet 变换的分解实例，其中图 1(a)大小为 512×512 的 Lena 图像，（b）为 Curvelet 变换分解的图像，(c)为小波变换分解的图像。

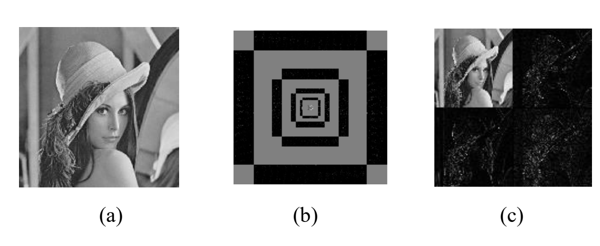


图 1 Curvelet 变换和小波变换实例

由图 1 可以看到，Lena 图像经过 Curvelet 变换后被划分为 6 个尺度层,第一层为 Coarse 尺度层,第六层即最外层为 Fine 尺度层，中间的第二至第五层为 Detail 尺度层，每层的系数分别被划分为 8、8、16、16 个小方向，都是由高频系数组成的矩阵。而 Lena 图像经过小波变换则被分成 4 个层，具体如图 1(c)所示。分别统计 Curvelet 变换和小波变换后每层系数的能量，将每层的系数的绝对值的平方和作为能量进行直方图对比，具体如图 2 所示。

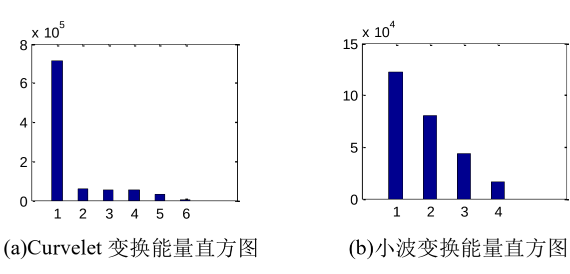


图 2 Curvelet 变换和小波变换能量直方图对比

其中图 2(a)(b)横向表示频域变换后的层数，纵向表示对应的能量。由图 2 的能量分布图可知，经 Curvelet 变换后的图像的系数能量主要集中于第一层，其余的各层分布的能量较少，而经过小波变换后的图像的能量分布 2、3 和 4 层（主要含有高频信息）的能量较多。

1.2 双奇异值分解（DSVD）

SVD 矩阵分析中常用的数学工具，它可以将一个矩阵分解为三个矩阵的乘积[13]，对于一个大小为 m×n 的矩阵 I，奇异值分解可表示为

$$I=U_{m\times n}\begin{bmatrix}\delta_1 & & & & \\ & \delta_2 & & & \\ & & \ddots & & \\ & & & \delta_{n-1} & \\ & & & & \delta_n\end{bmatrix}_{n\times n} V^T_{n\times m} \tag{5}$$

其中：$U_{m\times n}$ 左奇异矩阵，$\begin{bmatrix}\delta_1 & & & & \\ & \delta_2 & & & \\ & & \ddots & & \\ & & & \delta_{n-1} & \\ & & & & \delta_n\end{bmatrix}$ 为奇异值矩阵；$\delta_1\ge\delta_2\ge\cdots\ge\delta_{n-1}\ge\delta_n\ge 0$；$V^T_{n\times m}$ 为右奇异矩阵。图像经过奇异值分解会把冗余的信息去掉,用少量的奇异值代表整个图像的信息,在图像去噪和图像压缩具有重要的意义，同时经过奇异值分解后的图像具有一定抗攻击能力，所以经常用于数字水印领域来

提高算法的鲁棒性，但是传统奇异值分解的安全性较低且存在一定虚警问题[14]。

针对传统奇异分解存在的问题，提出一种具有安全性更高的双奇异值分解（DSVD）。DSVD 不直接对图像进行 SVD 分解，而且先对图像进行双对角化操作，然后对双对角矩阵进行奇异值分解。DSVD 分解过程如下：

a)先对矩阵 $I_{m\times n}$ 进行双对角化分解，如式(6)所示。

$$I_{m\times n}=U_I\,\Sigma_I\,V_I^T \tag{6}$$

其中：U_I 为正交矩阵；V_I^T 为酉矩阵。

$$\Sigma_I=\begin{bmatrix} I_{11} & I_{12} & & & \\ & I_{22} & I_{23} & & \\ & & \ddots & \ddots & \\ & & & I_{n-1,n-1} & I_{n-1,n} \\ & & & & I_{n,n} \end{bmatrix} \tag{7}$$

b)然后对得到的双对角矩阵 Σ_I 进行奇异值分解，得到最大奇异值矩阵：

$$\begin{cases}\Sigma_I=U_\Sigma S V_\Sigma^T \\ S=\max(\Sigma_I)\end{cases} \tag{8}$$

1.3 视觉密码

视觉密码是两位伟大的数学家 Moni Naor 和 Adi Shamir[15]提出的一种视觉系统解密的新型密码方案，它的核心思想是，将一个秘密图像（secret image），利用视觉密码加密规则加密，得到两张共享图份，其中第一张共享份可以看做是秘密图像加密后得到的密文（cipher）,第二张共享图份可以看做是解码的秘钥（key）。由于每一个共享份都是像随机噪声一样杂乱无章的，所以密码破译者是无法从一张图份中得到另一张共享份的任何信息的，更加无法破解秘密图像。

本文利用的视觉密码原理将水印信息产生两个密钥，将其中一个密钥进行 Arnold 置乱后与载体图像特征生成零水印，另一个密钥用于后期验证。其加密过程如式（9）～（10）所示。

$$\begin{bmatrix}1&1\\1&1\end{bmatrix}=\begin{cases}\begin{bmatrix}1&0\\0&1\end{bmatrix} & \begin{bmatrix}0&1\\1&0\end{bmatrix} & \begin{matrix}\text{key1}\\\text{key2}\end{matrix}\\ \begin{bmatrix}0&1\\1&0\end{bmatrix} & \begin{bmatrix}0&1\\1&0\end{bmatrix} & \end{cases} \tag{9}$$

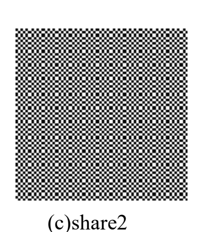
$$\begin{bmatrix}1&0\\0&1\end{bmatrix}=\begin{cases}\begin{bmatrix}1&0\\0&1\end{bmatrix} & \begin{bmatrix}0&1\\1&0\end{bmatrix} & \begin{matrix}\text{key1}\\\text{key2}\end{matrix}\\ \begin{bmatrix}1&0\\0&1\end{bmatrix} & \begin{bmatrix}0&1\\1&0\end{bmatrix} & \end{cases} \tag{10}$$

其中：两个密钥重叠得到$\begin{bmatrix}1&1\\1&1\end{bmatrix}$，则原始图像的像素为黑色像素，否则为白色像素。图 3 为视觉密码加密实例，其中图 3(a)为水印图像，(b)和(c)分别是通过视觉密码原理生成的两个互不重叠的密钥 share1 和 share2。



(a)版权水印

（b)share1



(c)share2

图 3　视觉密码实例

2　零水印算法

2.1　零水印生成

零水印的生成过程需要构造图像的特征信息，首先对大小为 512×512 图像进行 Arnold 置乱，然后对置乱后的图像进行 Curvelet 变换、分块和 DSVD，最后构造特征矩阵。同时对版权水印进行视觉密码加密生成两个共享份，将其中一个共享份进行 Arnold 置乱，最后将置乱后的共享份与特征矩阵进行异或操作生成零水印，将生成的零水印和另一共享份保存至版权保护中心。零水印具体生成步骤如下所示：

a)对大小为 512×512 的载体图像 I 进行 Arnold 置乱，置乱方式如式(11)所示。

$$\begin{pmatrix}x'\\y'\end{pmatrix}=\begin{bmatrix}1&1\\1&2\end{bmatrix}\begin{pmatrix}x\\y\end{pmatrix}\mathrm{mod}(N) \tag{11}$$

b)对置乱后的载体图像进行 Curvelet 变换，得到 Curvelet 变换的曲线系数矩阵 $cI_{256\times256}$。

c)然后按照式(12)对 $cI_{256\times256}$ 进行分块，得到块矩阵 B_k。

$$\begin{cases}IF\ \mathrm{mod}(i,4)==0\ \&\&\ \mathrm{mod}(j,4)==0 \quad Then\\ \quad B_{k\times k}\{i/4,j/4\}=cI(m,n)\end{cases} \tag{12}$$

其中：$i,j\in1,2,3\ldots256$；$m\in\{(i-3):(i)\},n\in\{(j-3):(j)\}$；$k\in1,2,3\cdots64$。

d)根据式(6)和(8)求得各个块 $B_{k\times k}$ 的最大奇异值 $S_{i,j}$，并构成最大奇异值矩阵 $S_{i,j}^{\max}$，然后根据式(13)求得最大奇异值矩阵的均值 M。

$$M=S_{i,j}^{\max}\Big/k\times k \tag{13}$$

e)利用每个块最大奇异值 $S_{i,j}^{\max}$ 与整体最大奇异值的均值 M 的关系构造特征矩阵 T。

$$T=\begin{cases}1 & IF\quad S_{i,j}^{\max}>M\\ 0 & ELSE\end{cases} \tag{14}$$

f)利用视觉密码原理对水印图像 W 进行加密操作，产生两个秘密图份 w_1 和 w_2，将其中一秘密图份 w_1 进行 Arnold 置乱，得到置乱后的秘密图份 w_{11}。

g)将 f)中置乱后的秘密图份 w_{11} 与 e)中得到的特征矩阵 T 进行异或操作生成零水印 Z，并将生成的零水印 Z 和秘密图份 w_2 存放于版权保护中心，两个置乱密钥 K_1 和 K_2 由客户保管。

$$Z=XOR(w_{11},T) \tag{15}$$

零水印产生过程如图 4 所示。

2.2　版权认证

版权认证过程需要从版权保护中心提取零水印 Z 和秘密图份 w_2,版权认证过程的曲线特征信息提取过程与 2.1 节的步骤 a)～e)一致得到新的特征矩阵 T'。具体步骤如下：

a)从版权保护中心得到零水印 Z 与新构造的特征矩阵 T' 进行异或操作得到置乱后秘密图份 w_{11}'。

$$w_{11}'=XOR(Z,T') \tag{16}$$

b)从客户中得到密钥 K_2 将秘密图份 w_{11}' 进行 Arnold 逆置乱，得到解密后的秘密图份 w_1'。

c)将解密后的秘密图份 w_1' 与版权中心的 w_2 进行重叠，得到版权水印 w_1'。

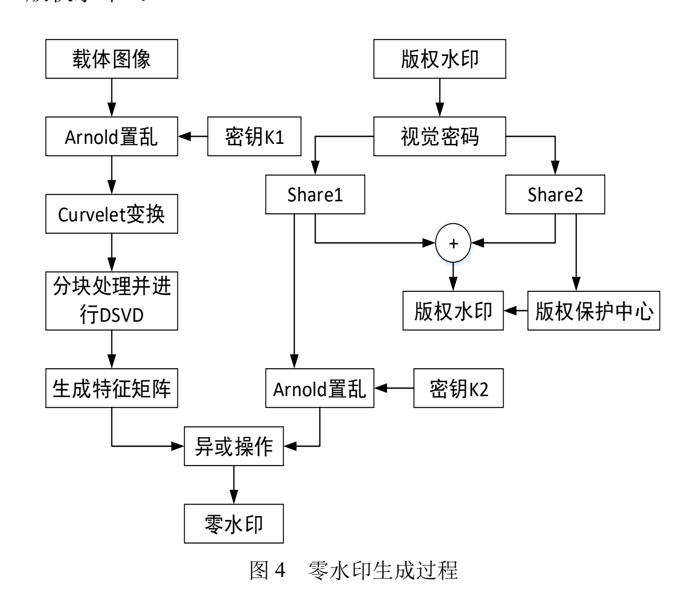


图 4　零水印生成过程

版权认证过程如图 5 所示。

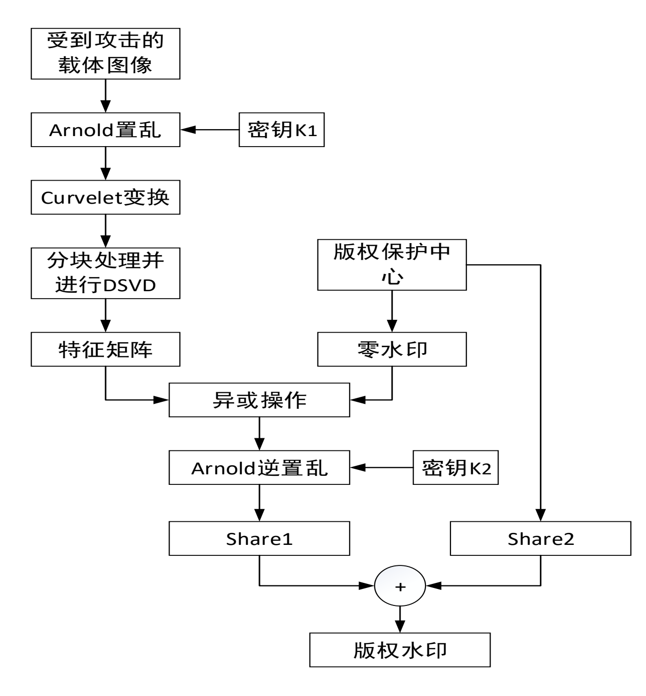
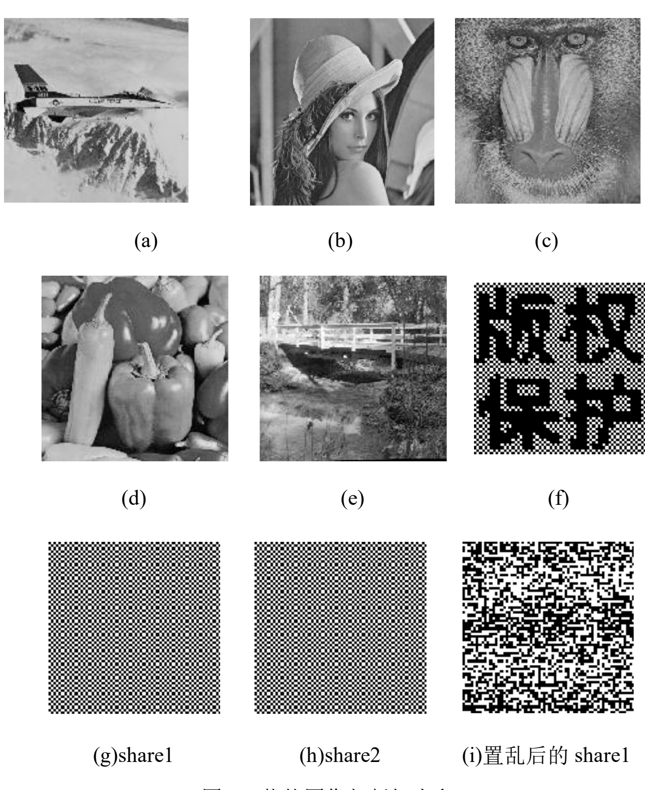


图 5　版权认证过程

3　参数说明及鲁棒性攻击实验

3.1　参数说明

为了验证本文算法的有效性，选择在 64 位 Windows7 操作系统和 MATLAB　R2014a 平台上进行仿真实验，实验载体图像选择大小为 512×512 的 Airplane、Lena、Baboon 、Paper 和 Bride 的标准灰度图像，分别对应图 6 (a)～（e）；版权水印图像选择大小为 64x64 含有”版权水印”四个字的二值水印图像，对应图 6 (f)；同时利用视觉密码将版权水印图像加密生成两个共享图份，分别对应图 6 (g)和(h)；为了进一步提高算法的安全性和鲁棒性，将得到的 share1 进一步置乱，用于增强算法的鲁棒性能，得到的置乱后的 share1，对应图 6(i)，具体如图 6 所示。



(a)　(b)　(c)　(d)　(e)　(f)　(g)share1　(h)share2　(i)置乱后的 share1

图 6　载体图像与版权水印

本文用归一化相关系数（NC）衡量提取的水印与原始水印相似度。NC 是衡量数字水印的相关标准，本文采用如下计算方式[16]：

$$NC(w,w')=\frac{\sum_{i=1}^{m}\sum_{j=1}^{n}w(i,j)w'(i,j)}{\sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n}w(i,j)^2}\sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n}w'(i,j)^2}} \tag{17}$$

其中：w 、w' 分别表示初始水印和提取的水印。

3.2　虚警率实验

为了验证算法的虚警问题，计算图 6 的五幅载体图像构造的零水印之间的相似性，不同零水印之间相似度越低，表明虚警率越低，否则相反。具体实验结果如表 1 所示。

表 1　虚警实验结果(NC 值)

偏移参数	Airplane	Lena	Baboon	Paper	Bride
Airplane	1.0000	0.5777	0.4952	0.4849	0.5667
Lena	0.5777	1.0000	0.4852	0.4480	0.4385
Baboon	0.4952	0.4852	1.0000	0.5337	0.5184
Paper	0.4849	0.4480	0.5337	1.0000	0.4847
Bride	0.5667	0.4385	0.5184	0.4847	1.0000

由表 1 可知，五幅不同载体图像之间生成的零水印的相似度都很低，最高相似度为 0.577 7，最低相似度为 0.438 5，平均相似度为 0.503 3，表明本文算法虚警较低。

3.3　非几何鲁棒攻击实验

常见的非几何鲁棒性攻击主要为噪声攻击、滤波攻击和压

缩攻击等。本文实验主要围绕以上几种非几何攻击进行鲁棒性攻击实验。

1）噪声攻击

本文对五幅不同的载体图像进行的不同强度的椒盐噪声攻击检验算法对于不同强度噪声的抵抗能力，并计算提取水印的NC 值。具体实验结果如表 2 所示。

表 2　不同强度椒盐噪声攻击实验数据表(NC 值)

噪声强度	Airplane	Lena	Baboon	Paper	Bride
0.1	0.9751	0.9769	0.95087	0.9838	0.9709
0.2	0.9531	0.9612	0.9463	0.9549	0.9518
0.3	0.9308	0.9436	0.9102	0.9399	0.9296
0.4	0.9288	0.9103	0.9038	0.9198	0.9086
0.5	0.8846	0.8938	0.8601	0.89335	0.8865

由表 2 可以看出，随着噪声强度的增大，从五幅载体图像中提取的水印与原始版权水印的相似度（NC 值）都很高，平均值在 0.910 0 以上。对于载体图像 Lena 对于以上各种强度的椒盐噪声攻击时得到的 NC 值最高为 0.976 9，最低为 0.893 8。而对于载体图像 Airplane、Baboon、Paper 和 Bride 得到的 NC 值的平均值也在 0.912 3 以上。对于以上几种不同强度的椒盐噪声攻击，整体表现出较好的鲁棒性能。

2)JPEG 压缩攻击

对五幅载体图像进行不同强度的 JPEG 压缩攻击，压缩攻击主要去除载体图像的冗余的信息，载体图像在受到压缩攻击后，生成的零水印也因此受到较大的影响。具体实验数据如表 3 所示。由表 3 可知，对于不同的压缩强度攻击，从五幅载体图像中提取的水印与原水印的相似度的平均值为 0.994 5 以上，表明本文算法对不同强度的 JPEG 压缩攻击表现出较强的鲁棒性能。

表 3　不同强度 JPEG 压缩攻击实验数据表(NC 值)

压缩因子	Airplane	Lena	Baboon	Paper	Bride
10	0.9909	0.9922	0.9778	0.9935	0.9904
20	0.9939	0.9939	0.9839	0.9974	0.9918
30	0.9961	0.9974	0.9874	0.9974	0.9935
40	0.9970	0.9961	0.9848	0.9983	0.9926
50	0.9957	0.9961	0.9918	0.9987	0.9944
60	0.9974	0.9987	0.9927	0.9987	0.9939

3)中值滤波攻击

对五幅载体图像分别进行中值滤波攻击，选择的模板大小分别为 3×3、5×5、7×7 和 9×9 的滤波模板进行仿真实验。具体实验数据如表 4 所示。由表 4 可知，五幅载体图像在受到不同的滤波攻击后，得到 NC 值在 0.963 7～0.999 1，即使是 9×9 的滤波模板得到的 NC 值的平均值也在 0.981 3 以上。所以本文算法对以上四种不同模板大小的中值滤波攻击具有较强的抵抗攻击能力。

表 4　中值滤波攻击实验数据表(NC 值)

模板大小	Airplane	Lena	Baboon	Paper	Bride
3×3	0.9965	0.9974	0.9852	0.9991	0.9926
5×5	0.9917	0.9948	0.9769	0.9970	0.9865
7×7	0.9891	0.9926	0.9708	0.9957	0.9791
9×9	0.9856	0.9909	0.9637	0.9913	0.9751

3.4　几何鲁棒攻击实验

几何攻击主要为旋转攻击和行列偏移攻击，几何攻击使得载体图像发生很大的变化，所以对提取的水印影响也较大。

1)旋转攻击

实验对五幅载体图像分别进行小幅度的旋转攻击，旋转角度分别为 1°、2°和 3°。具体实验数据如表 5 所示。由表 5 可以看出，本文算法对于旋转攻击表现出较好的鲁棒性能。

表 5　旋转攻击实验数据表（NC 值）

旋转度数	Airplane	Lena	Baboon	Paper	Bride
向左 1°	0.9850	0.9838	0.9816	0.9833	0.9816
向右 1°	0.97981	0.9738	0.9838	0.9887	0.9724
向左 2°	0.9417	0.9516	0.9466	0.9427	0.9416
向右 2°	0.9465	0.9423	0.9537	0.9403	0.9430
向左 3°	0.9300	0.9369	0.9376	0.9280	0.9288
向右 3°	0.9321	0.9281	0.9325	0.9363	0.9348

2）行列偏移攻击

对五幅载体图像分别进行上、下、左、右四个方向进行不同行列的移动攻击,移动丢失的像素进行置 0 操作。具体实验数据如表 6 所示。由表 6 可知，对五幅载体图像偏移 2 列时，提取的水印 NC 值在 0.967 1 以上。而偏移 5 行时，得到的 NC 值最低为 0.923 6，最高为 0.9506。由于 Curvelet 变换具有多尺度、多方向性，所以对于各个方向的攻击时，依然能够很好地提取水印信息，说明本文算法对于抵抗各个方向的行列偏移攻击表现出的鲁棒性较强，

表 6　行列偏移攻击实验结果（NC 值）

偏移方向	偏移参数	Airplane	Lena	Baboon	Paper	Bride
向左	2 列	0.9673	0.9756	0.9707	0.9698	0.9638
偏移	5 列	0.9326	0.9496	0.9239	0.9243	0.9416
向右	2 列	0.9716	0.9723	0.9671	0.9673	0.9695
偏移	5 列	0.9260	0.9482	0.9226	0.9206	0.9361
向上	2 行	0.9718	0.9792	0.9711	0.9835	0.9726
偏移	5 行	0.9251	0.9430	0.9236	0.9496	0.9420
向下	2 行	0.9846	0.9809	0.9712	0.9738	0.9752
偏移	5 行	0.9331	0.9506	0.9341	0.9459	0.9413

3.5　组合攻击

为了进一步验证算法的强鲁棒性能，本文增加组合攻击仿

真实验，组合攻击的类型分别为旋转攻击+噪声攻击、JPEG 压缩攻击+噪声攻击、JPEG 压缩攻击+中值滤波攻击、行列偏移攻击+中值滤波攻击和行列偏移攻击+高斯噪声攻击等。具体实验数据如表 7 所示。由表 7 可知，对于 JPE 压缩 30%+中值滤波，载体图像 Airplane、Lena、Paper 和 Bride 得到的 NC 值都在 0.991 3 以上。对于 JPEG 压缩 30%+高斯噪声 0.05 攻击时，整体得到的 NC 值的平均为 0.966 8。总体而言，本文算法对于以上几种组合攻击表现出较强的鲁棒性能。

表 7　组合攻击实验数据表（NC 值）

攻击类型	Airplane	Lena	Baboon	Paper	Bride
向左旋转 2°+椒盐噪声 0.05	0.9368	0.9312	0.9261	0.9248	0.9213
JPEG 压缩 30%+高斯噪声 0.05	0.9685	0.9756	0.9611	0.9709	0.9582
JPEG 压缩 30%+中值滤波 3x3	0.9935	0.9970	0.9822	0.9956	0.9913
向下偏移 2 行+中值滤波 5x5	0.9709	0.9792	0.9606	0.9839	0.9766
向右偏移 2 列+高斯噪声 0.05	0.9505	0.9556	0.9931	0.9561	0.9526

3.6　对比实验

为了更好地验证本文算法的鲁棒性能，选择大小为 512×512 的 Lena 图像作为载体图像，水印图像选择大小为 64×64 含有“版权水印”的二值图像与文献[4,8,9]进行实验对比，具体不同攻击类型与实验结果如表 8 所示。

1)鲁棒性分析

由表 8 可知，本文算法对于抵抗非几何攻击和几何攻击相比于文献[4,8,9]表现出的鲁棒性能更优秀。对于非几何攻击，当噪声强度为 0.2 时，文献[4]得到的 NC 值为 0.804 0，鲁棒性较差。 椒盐噪声攻击如图 7 所示。由图 7 可以看出，随着噪声强度越来越大，本文算法的 NC 值一直比文献[4,8,9]的要高。JPEG 压缩攻击如图 8 所示。从图 8 可以看出，在不同的 JPEG 压缩强度下，文献[8,9]与本文算法得到的 NC 值几乎一致，而对比文献[4]具有较大的提升。由于文献[4,8,9]使用的小波变换具有局部局限性，不具有方向性，在受到非几何攻击时，图像边缘信息常常被削弱。本文算法所使用的 Curvelet 变换和 DSVD 有效地增强了算法的鲁棒性，因为 Curvelet 变换对图像边缘信息起到了增强的效果，相比于小波变换对于图像的边缘信息具有更强的表现能力，所以图像在受到非几何攻击时鲁棒性更强。

对于几何攻击，相比文献[4,8,9]具有较大的提升，尤其在剪切攻击和旋转攻击方面，在剪切攻击方面本文算法比文献[9]提升 6%左右。旋转攻击如图 9 所示。从图 9 可以看出，对于不同角度的旋转攻击，本文算法的 NC 值一直比文献[4,8,9]的要高，平均高出 5%左右，而向左旋转 3º 时，本文的 NC 值在 0.93 左右，文献[4,8,9]的 NC 值都 0.9 以下，鲁棒性较差。对于行列偏移攻击，相比文献[4,8,9]提升%2-9%。文献[4]使用块最大奇异值构成图像的特征，在像素位置发生变化时，块的最大奇异值也会产生较大的变化。文献[8]使用 DCT 的均值构造的零水印，在受到剪切操作时，图像块均值影响较大。而文献[9]直接在空域中利用块均值与整体均值的关系构造特征矩阵，在受到几何攻击时，图像的像素或像素的位置发生了变化，直接影响了块均值与整体均值的关系，稳定性较差。本文使用的块最大奇异值与整体最大奇异值构造特征，最大奇异值具有能量集中稳定性能，相比文献[4,8,9]具有稳定性更高。总体而言，本文算法对于常规的鲁棒性攻击要比文献[4,8,9]的更具有优势，鲁棒性更强。

表 8　本文算法与文献[4,8,9]对比实验数据表(NC 值)

攻击类型	参数	文献[4]	文献[8]	文献[9]	本文算法
椒盐噪声	0.05	0.9140	0.9738	0.9739	0.9878
	0.2	0.8062	0.9478	0.9365	0.9612
高斯噪声	0.05	0.9454	0.9585	0.9949	0.9843
	0.2	0.8040	0.9144	0.9707	0.9631
中值滤波	模板大小 3x3	0.9819	0.9766	0.9971	0.9974
高斯滤波	模板大小 3 x 3	0.9832	0.9782	0.9949	0.9965
JPEG 压缩	压缩因子 10	0.9300	0.9917	0.9895	0.9922
	压缩因子 30	0.9707	0.9913	0.9927	0.9935
剪切攻击	左上角 1/16	0.9587	0.9357	0.8712	0.9389
	右下角 1/16	0.9590	0.9295	0.8812	0.9300
旋转攻击	向左旋转 3°	0.8893	0.8772	0.8474	0.9369
	向右旋转 3°	0.8818	0.86677	0.8662	0.9281
行列偏移	下移 2 行	0.9033	0.9597	0.9668	0.9809
	右移 2 列	0.8803	0.9516	0.9597	0.9723
缩放攻击	先缩小 0.5 倍再放大 2 倍	0.9924	0.9984	0.9984	0.9988
	先放大 4 倍再缩小 0.25 倍	0.9982	0.9991	0.9993	0.9995

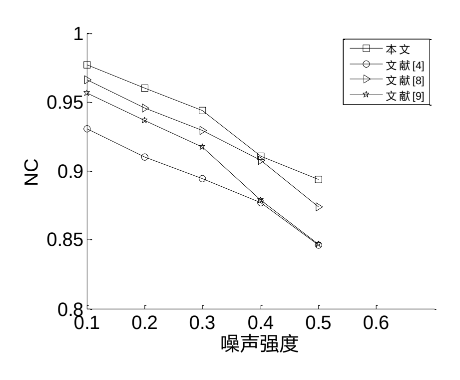


图 7　椒盐噪声攻击

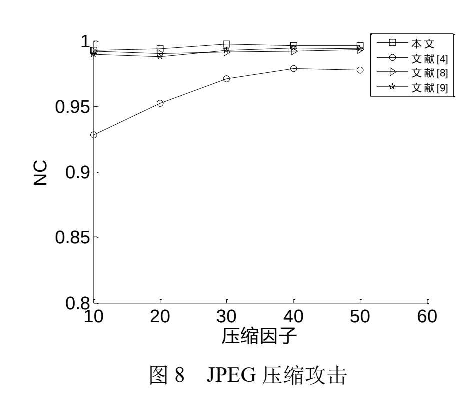


图 8　JPEG 压缩攻击

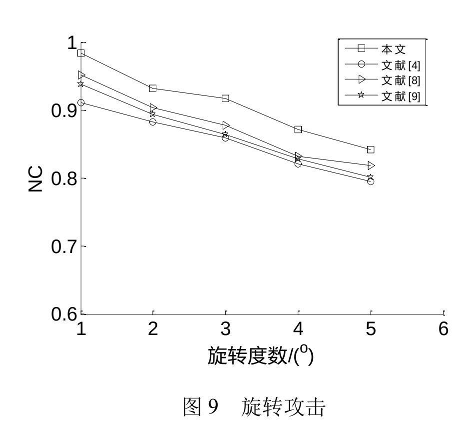


图 9　旋转攻击

2)安全性分析

在安全性能方面，本文算法相比文献[4,8,9]更安全，文献[4,8,9]只使用传统的加密操作，安全性较低。本文算法在提取特征过程中对载体图像进置乱操作，一是消除图像像素间的相关性，二是加强算法的安全性,攻击者在对载体图像进行特征提取时，在不知道特征提取的密钥情况下是很难提取到一致的特征信息。同时使用视觉密码和 Arnold 置乱方式对水印信息进行加密处理，生成的零水印并不是直接由版权水印构造的，而是利用视觉密码产生的共享图份进行构造，由于共享图份是一张类似噪声点的密钥图份，所以即使获得零水印信息也无法得知其中的版权信息。

4　结束语

本文基于 Curvelet 变换、DSVD 和视觉密码理论提出一种基于 Curvelet-DSVD 和视觉密码的强鲁棒零水印算法，该算法克服了传统零水印算法不能表征自然图像曲线特征和对于较大强度攻击鲁棒性差的问题。同时，视觉密码实现将版权水印一分为二，实现三方认证方式，Arnold 变换对视觉密码的共享份进行置乱，进一步提高了水印的安全性。实验结果表明，该算法对于常规的噪声攻击、滤波攻击、压缩攻击、旋转攻击、行列偏移攻击表现出较强的鲁棒性能，同时算法的安全性较高。但本文算法对于较大强度的组合攻击时表现的鲁棒性稍差，有待进一步的优化，在下一步的研究中，将进一步提高算法对于复杂环境中的抗攻击能力。

参考文献：

[1] 温泉，孙铁锋，王树勋. 零水印的概念与应用 [J]. 电子学报, 2003, 31 (2): 214-216.

[2] 吴伟民，丁冉，林志毅，等. 基于混沌的医学图像窜改定位零水印算法 [J]. 计算机应用研究, 2014, 31 (12): 3685-3688.

[3] Rao Y R, Nagabhooshanam E. A novel image zero-watermarking scheme based on DWT-BN-SVD [C]// Proc of International Conference on Information Communication and Embedded Systems. 2014: 1-6.

[4] Rani A, Bhullar A K, Dangwal D, et al. A zero-watermarking scheme using discrete wavelet transform [J]. Procedia Computer Science, 2015, 70: 603-609.

[5] Liu P, Tan Y. Robust zero-watermarking algorithm based on invariant centroid [C]// Proc of International Conference on Computational and Information Sciences. 2013: 758-761.

[6] 陈伟琦，李倩. 基于 DWT-SVD 的图像双零水印算法 [J]. 计算机工程与科学, 2014, 36 (10): 1991-1996.

[7] Zhang L, Cai P, Tian X, et al. A novel zero-watermarking algorithm based on DWT and edge detection [C]// Proc of the 4th International Congress on Image and Signal Processing. 2011: 1016-1020.

[8] 赵杰. 基于 DCT 均值的图像零水印算法 [J]. 系统仿真技术, 2015, 11 (4): 304-306.

[9] 曾文权，熊祥光. 基于整数小波变换的鲁棒零水印算法 [J]. 微电子学与计算机, 2016, 33 (4): 97-101.

[10] 曲长波，李栋栋. 基于视觉密码和边缘检测的零水印算法 [J]. 计算机应用与软件, 2016, 33 (9): 328-333.

[11] 肖振久，张晗，陈虹，等. 增强奇异值分解和细胞神经网络的零水印 [J]. 中国图象图形学报, 2017, 22 (3): 288-296.

[12] 汪太月，李宏伟，李志明. 基于 Curvelet 变换的数字水印算法 [J]. 数学的实践与认识, 2012, 42 (17): 124-128.

[13] 何冰. 基于 SVD 和 Radon 变换的抗旋转攻击盲水印算法 [J]. 计算机工程与应用, 2012, 48 (20): 200-205.

[14] Srilakshmi P, Himabindu C. Image watermarking with path based selection using DWT & SVD [C]// Proc of International Conference on Computational Intelligence and Computing Research. 2016: 1-5.

[15] Naor M, Shamir A. Visual cryptography [C]// Advances in Cryptology-Eurocrypt’94. 1995: 1-12.

[16] 曲长波，杨晓陶，袁铎宁. 小波域视觉密码零水印算法 [J]. 中国图象图形学报, 2014, 19 (3): 365-372.